

1 ERIC A. GROVER (SBN 136080)
 2 eagrover@kellergrover.com

2 RACHAEL G. JUNG (SBN 239323)
 3 rjung@kellergrover.com

3 **KELLER GROVER LLP**

4 1965 Market Street
 5 San Francisco, California 94103
 Telephone: (415) 543-1305
 Facsimile: (415) 543-7861

6 SCOT BERNSTEIN (SBN 94915)
 7 swampadero@sbernsteinlaw.com

8 **LAW OFFICES OF SCOT D. BERNSTEIN,
 A PROFESSIONAL CORPORATION**
 9 101 Parkshore Drive, Suite 100
 Folsom, California 95630
 Telephone: (916) 447-0100
 Facsimile: (916) 933-5533

10 *Attorneys for Plaintiffs*
 11 Ryan Wu and Saber Khamooshi

12
 13 **UNITED STATES DISTRICT COURT**
 14 **NORTHERN DISTRICT OF CALIFORNIA**

15
 16 RYAN WU and SABER KHAMOOSHI,) Case No: 3:24-cv-05150-MMC
 17 individually and on behalf of a class of)
 similarly situated individuals,) **CLASS ACTION**
 18 Plaintiffs,)
 19 v.) **SECOND AMENDED COMPLAINT
 20 GANNETT CO., INC.; and DOES 1 through) FOR DAMAGES**
 100, inclusive,)
 21 Defendants.) **DEMAND FOR JURY TRIAL**
 22) Action Filed: June 26, 2024
 23) FAC Filed: July 23, 2024
 24
 25
 26
 27
 28

CLASS ACTION COMPLAINT

Plaintiffs Ryan Wu and Saber Khamooshi, on behalf of themselves and a class of similarly situated individuals as defined below, and based on personal knowledge where applicable, information and belief, and investigation by counsel, allege the following against Defendant Gannett Co., Inc.

INTRODUCTION

1. This class action lawsuit arises out of Defendant's policy and practice of embedding and using various trackers on Defendant's USA Today website, www.usatoday.com, to (1) install and store third-party tracker cookies on California website users' browsers and (2) collect California website users' browser and device/operating system data as well as personally identifying and addressing information, such as IP addresses¹, that the USA Today website then surreptitiously discloses to and shares with the third-party trackers without users' knowledge, authorization, or consent.

2. Defendant Gannett Co., Inc. ("Defendant" or "Gannett") is an American mass media company that owns and publishes various brands that deliver journalism, compelling content, events, experiences, and digital marketing business solutions. Gannett's portfolio includes hundreds of brands and local media outlets across the United States and United Kingdom, including USA Today, The Arizona Republic, Golfweek, Newsquest Media Group, and many others. Gannett also owns and operates a number of daily newspapers in California that provide local news stories, content, and relevant local advertising, including The Desert Sun, The Salinas Californian, Visalia Time-Delta, Record Searchlight, Ventura County Star, Victorville Daily Press, Tulare Advance Register, and The Stockton Record.

3. Founded in 1980 and launched in 1982, USA Today is a newspaper and news broadcasting company that operates from Gannett's corporate headquarters in New York. USA

¹ IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Department of Health and Human Services (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>

1 Today covers breaking news, politics, sports, entertainment, money, wellness and more. Its
2 newspaper is printed at 37 sites across the United States, including at one production facility in
3 California, and at five additional sites internationally. Defendant also owns and operates the
4 www.usatoday.com website (the “USA Today website”), which provides breaking news and
5 coverage of U.S. and national news.

6 4. Plaintiffs and Class members who visit the USA Today website expect that their
7 personally identifying information, including their IP addresses, will remain private and confined
8 to their use of the USA Today website. Plaintiffs and Class members have a reasonable
9 expectation that their accessing of and interactions with the USA Today website will not be shared
10 with any third parties, let alone with *undisclosed* third-party trackers, or sold for advertising
11 purposes.

12 5. Unbeknownst to individuals entering and viewing the USA Today website, third-
13 party trackers are embedded into Defendant’s website. Through that embedded tracking
14 technology, while Plaintiffs and Class members were and are accessing and interacting with the
15 USA Today website, Defendant (1) installed and stored and continues to install and store third-
16 party tracker cookies on users’ browsers and (2) captured and continues to capture USA Today
17 website users’ browser and device/operating system data, IP addresses, and other identifying
18 information. All of this happens the moment users enter the USA Today website and without any
19 further action required by or requested of the users.

20 6. Plaintiffs are informed and believe and, on that ground, allege that Defendant
21 surreptitiously shares identifying data, including addressing information such as IP addresses, with
22 the third-party trackers for advertising and analytics-related purposes. Defendant does so without
23 obtaining USA Today website users’ authorization or consent and without a court order.

24 7. Defendant’s unauthorized (1) installation of third-party tracker cookies on
25 California users’ web browsers and (2) collection and disclosure to third parties of Plaintiffs’ and
26 Class members’ personally identifying and addressing information, all without consent or adequate
27 notification to Plaintiffs and Class members, are invasions of Plaintiffs’ and Class members’
28 privacy. Defendant’s actions also violate various laws, including the California Computer Data

1 Access and Fraud Act, Cal. Penal Code § 502 (“CDAFA”); the California Invasion of Privacy Act,
2 Cal. Penal Code §§ 630, *et seq.* (“CIPA”); and the right to privacy under Article 1, § 1, of the
3 California Constitution. The latter includes privacy as one of six fundamental rights of all
4 Californians.

5 **PARTIES**

6 **A. Plaintiffs Ryan Wu and Saber Khamooshi**

7 8. Plaintiffs are natural persons and residents of California.

8 9. While physically present in California, Plaintiff Wu regularly has visited and still
9 visits the USA Today website to browse news headlines and read articles. He visited the USA
10 Today website as recently as May 2024. Plaintiff Wu used and continues to use an internet browser
11 on his computer and on his cellular phone to access Defendant’s website.

12 10. While physically present in California, Plaintiff Khamooshi regularly has visited
13 and still visits the USA Today website to browse news headlines and read articles. He visited the
14 USA Today website as recently as June 2024. Plaintiff Khamooshi used and continues to use an
15 internet browser on his computer and on his cellular phone to access Defendant’s website.

16 11. At no time when either Plaintiff entered the USA Today website and viewed its
17 content did either Plaintiff authorize Defendant to install or consent to Defendant installing third-
18 party tracker cookies on his internet browser or computer.

19 12. Plaintiffs also did not consent to Defendant sharing and selling their browser and
20 device/operating system data, IP addresses and other personally identifying information with or to
21 third-party trackers. Further, because Defendant did not provide notice or request permission,
22 Plaintiffs were unaware of and had no meaningful opportunity to opt out of or object to that
23 unauthorized disclosure of their data.

24 **B. Defendant Gannett Co., Inc., and the USA Today Website**

25 13. Defendant Gannett Co., Inc. is a corporation organized under the laws of the State
26 of Delaware with its headquarters and principal place of business in New York, New York.
27 Defendant systematically and continuously does business in California and with California
28 residents.

1 14. In parallel with its national publications, Defendant also owns and operates local
2 brands, *including eight daily publications in California*:

- 3 (a) The Desert Sun in Palm Springs, California;
- 4 (b) The Salinas Californian in Salinas, California;
- 5 (c) Visalia Times-Delta in Visalia, California;
- 6 (d) Redding Record Searchlight in Redding, California;
- 7 (e) Ventura County Star in Camarillo, California;
- 8 (f) The Stockton Record in Stockton, California;
- 9 (g) Victorville Daily Press in Victorville, California; and
- 10 (h) Tulare Advance Register in Tulare, California.

11 15. The website for each of these California daily publications states that the local
12 brand is a part of the USA TODAY Network and is owned and operated by Gannett Co., Inc.

13 16. Each of the California daily publications covers local content specific to its area
14 under the headings “Local News” and “More Local News.” The website for each also publishes
15 national content that is shared between and among Defendant’s numerous brands. In addition to
16 the local news, the website for each California publication has a “Marketplace” for local
17 advertisements, classified advertisements, and public notices.

18 17. Defendant’s California-centered websites also state proudly that they support local
19 businesses in a number of cities, including four large cities in California: San Francisco (156
20 businesses); Los Angeles (151 businesses); Palm Desert (150 businesses); and Redding (139
21 businesses). After choosing a California city under the “Support Local Businesses” link, the
22 website displays an alphabetical list of local businesses supported, their contact information, and
23 a link that redirects a user to the website of the local California business.

24 18. To carry out its numerous business activities inside of California, Gannett employs
25 individuals within and around California. At the end of September 2024, under the “Careers” tab
26 on the Gannett website, there were at least 10 job postings listed in California in six different cities,
27 including Stockton, Palm Springs, Camarillo, Visalia, Sacramento, and Victorville, to add to

28

1 Gannett's California workforce.²

2 19. Similarly, Defendant maintains various offices throughout California, including a
 3 corporate office in Los Angeles with departments for Sales, Accounting, Engineering, Marketing
 4 and Business Development, among others. Gannett also has a retail office in San Francisco,
 5 California, to handle sales, marketing and business development. A number of the California daily
 6 publications also have offices in cities such as Palm Desert, Palm Springs, Redding, and Salinas.

7 20. As part of its mass-media holdings, Defendant currently owns and operates USA
 8 Today and its website, www.usatoday.com. That website publishes breaking news, politics, sports,
 9 entertainment, money-related articles, wellness and more from across the country and around the
 10 world.

11 21. Defendant's USA Today website fails to put visitors on notice of Defendant's use
 12 of website tracking technology, including its use of third-party trackers. Upon information and
 13 belief, Plaintiffs allege that third-party trackers allow and enable companies like and including
 14 Defendant to sell advertising space on their websites by using the tracking technology to receive,
 15 store and analyze information surreptitiously collected from website visitors.

16 22. The USA Today website also failed and fails to disclose the selling and sharing of
 17 browser and device/operating system data and personally identifying information, including IP
 18 addresses and other addressing information, to and with unauthorized third party-trackers for
 19 advertising and other purposes.

20 **C. Doe Defendants**

21 23. Plaintiffs are ignorant of the true names and capacities of defendants sued herein as
 22 DOES 1 through 100, inclusive, and therefore sue those defendants by those fictitious names.
 23 Plaintiffs will amend this Complaint to allege those defendants' true names and capacities when
 24 ascertained. Plaintiffs are informed and believe and, on that ground, allege that each of the
 25 fictitiously-named defendants is responsible in some manner for the occurrences alleged in this
 26 Complaint and that Plaintiffs' injuries and damages, as alleged, are proximately caused by those

28 ² Search Jobs, Gannett, <https://www.gannett.com/search-jobs/> (last visited September 30, 2024).

1 occurrences.

2 24. Plaintiffs are informed and believe and, on that ground, allege that at all relevant
3 times, all named Defendants and the Doe Defendants were the principals, agents, partners, joint
4 venturers, officers, directors, controlling shareholders, controlling persons, subsidiaries, affiliates,
5 parent corporations, successors in interest, and/or predecessors in interest of some or all of the
6 other Defendants, were engaged with some or all of the other Defendants in a joint enterprise for
7 profit, and bore such other relationships to some or all of the other Defendants as to be liable for
8 their conduct with respect to the matters alleged below. Plaintiffs are informed and believe and,
9 on that ground, allege that each Defendant acted pursuant to and within the scope of the
10 relationships alleged above and that each knew or should have known about, and that each
11 authorized, ratified, adopted, approved, controlled, and aided and abetted the conduct of all
12 Defendants.

13 **JURISDICTION AND VENUE**

14 25. This Court has subject matter jurisdiction over this action under the California
15 Computer Data Access and Fraud Act, Cal. Penal Code §502, the California Invasion of Privacy
16 Act, Cal. Penal Code § 638.51, and the California Constitution.

17 26. This Court has personal jurisdiction over the parties because Defendant has
18 sufficient minimum contacts with this State in that it operates its numerous brands and businesses
19 within and markets its services and products throughout the State. As described in Paragraphs 14
20 through 19, Defendant's activities in California are substantial, continuous, and systematic. In
21 addition to its production facility located in California, Defendant owns and operates eight
22 California daily newspapers, each focusing on local news and content, promoting local California
23 businesses, and serving local regional advertisements. To conduct its numerous business activities
24 within California and support its local brands, Defendant employs California residents and
25 maintains offices in various cities throughout California. In describing its local brands,
26 Defendant's website states: ***“For the community, by the community. Our local brands are
27 engrained in the places we call home.”***

28 27. In addition to its media holdings in California, Defendant also owns a number of

1 subsidiaries that are either incorporated in or organized under the laws of the State of California.
 2 These include Defendant's digital marketing services companies under the brand LocaliQ.
 3 LocaliQ is headquartered in Woodland Hills, California and has sales and other offices in Irvine,
 4 Los Angeles, and San Francisco, California, as well as in Texas. Defendant's other California
 5 subsidiaries, which are organized under California law, include Salinas Newspapers LLC,
 6 SureWest Directories, The Desert Sun Publishing Co., The Sun Company of San Bernardino,
 7 California, and Visalia Newspapers LLC.

8 28. Further, a substantial part of the events and conduct giving rise to Plaintiffs' claims
 9 occurred in the State of California. Those events and that conduct included Plaintiffs' accessing
 10 of and interactions with the USA Today website, Defendant's unauthorized installation of third-
 11 party tracker cookies on California users' web browsers, and the collection and surreptitious
 12 sharing of Plaintiffs' and Class members' browser and device/operating system data and
 13 personally identifying and addressing information with the third-party trackers, all without users'
 14 knowledge, authorization or consent. Plaintiffs' rights were violated in the State of California, and
 15 those violations arose out of their contact with Defendant from and within the State of California.

16 29. Venue is proper in this Court because Defendant removed the action from San
 17 Francisco County Superior Court. Venue was proper in that court under Code of Civil Procedure
 18 §§ 395 and 395.5 and case law interpreting those sections, which provide that if a foreign business
 19 entity fails to designate with the office of the California Secretary of State a principal place of
 20 business in California, it is subject to being sued in any county that a plaintiff desires. On
 21 information and belief, Defendant Gannett Co., Inc. is a foreign business entity and had failed to
 22 designate a principal place of business in California with the office of the Secretary of State as of
 23 the date on which the Complaint in this action originally was filed.

FACTUAL ALLEGATIONS COMMON TO THE CLASS

A. Website Tracking Technology

26 30. Trackers collect information about internet users while those users are browsing the
 27 web. Trackers use cookies, scripts or pixels inserted by publishers or advertisers. Tracker profiling
 28 is the process of linking data from different websites to build user profiles based on the users'

1 browsing history, to place those users into categories or groups, and to sell that data to third parties
2 to use for targeted advertising.

3 31. A broad range of online technologies track and monitor internet-based interactions
4 and communications. Four identifier tools that commonly are used are (i) website cookies, (ii)
5 tracking pixels, (iii) digital fingerprinting and (iv) software development kits.

6 32. A website cookie refers to a small text file that a website server creates and
7 transmits to a web browser (e.g., Google Chrome or Safari) which then installs and stores the file
8 in a particular directory on an individual's computer, phone or other device.³ When a website user
9 attempts to access a webpage, the user's browser transmits a communication to the website's server
10 requesting that the server display the website's content for the browser to load. While providing
11 the requested content to the user, the website's server also provides the cookies that it would like
12 the user's browser to install and retain.

13 33. Website cookies contain information that identifies the domain name of the
14 webserver that wrote the cookie (e.g., www.hulu.com or www.facebook.com). Cookies also have
15 information about the user's interaction with a website, such as how the website should be
16 displayed, how many times a user has visited the website, how long a user spends on a webpage,
17 information about what pages the user visited, and authentication information. In addition to a
18 unique identifier and a site name, website cookies also can include personally identifiable
19 information such as a user's name, address, email address or telephone number if that information
20 was provided to a website.

21 34. A first-party cookie is implemented by the website that the user accesses. The
22 website uses its cookies for authentication, monitoring user sessions, and collecting analytical data.
23 A third-party cookie, also called an "advertising cookie" or a "tracker cookie," is a cookie that
24 belongs to a domain other than the one being displayed to the user in his or her browser. A third-
25 party cookie typically is used for cross-site tracking, retargeting and ad-serving. The key

26
27
28 ³ See Sara J. Nguyen, *What Are Internet Cookies and How Are They Used?* All About Cookies
(Jul. 28, 2023), <https://allaboutcookies.org/what-is-a-cookie>.

1 differences between the first-party and third-party cookies are who sets them (*i.e.*, a website
 2 display host or a third party), whether and how they can be blocked by a web browser, and the
 3 availability of the cookie. A third-party advertising or tracker cookie is available and accessible
 4 on *any* website that loads the third-party server's code, not just on the host website that the user is
 5 trying to access.

6 35. A pixel, also known as a “tracking pixel,” “web bug,” “clear GIF” or “web beacon,”
 7 is similar to a website cookie. It is a small, almost invisible image (pixel) embedded in a website
 8 or an email to track a user’s activities. That tracked data often includes information regarding the
 9 user’s operating system, the type of website or email used, the time when the website was accessed,
 10 the user’s IP address, and whether there are cookies that previously have been set by the server
 11 hosting the pixel image.⁴

12 36. “Digital fingerprinting” refers to device fingerprinting and browser fingerprinting,
 13 both of which send information to the website server to help ensure that a website is displaying
 14 content correctly and operating appropriately. Although a browser or device does not usually
 15 transmit personal information about a user, most fingerprinting is performed via a third-party
 16 tracker. ***A third-party tracker can track an individual across multiple sites and form a profile of***
 17 ***the user.***⁵

18 37. A software development kit (“SDK”) is a set of computer programs and similar
 19 tools that developers and engineers can leverage to build applications for specific platforms. The
 20 SDK often includes, among other tools, libraries, application programming interfaces, instructions,
 21 guides, directions, and tutorials.⁶ SDKs also may have embedded code that allows them to
 22 intercept personal data and other information from application users surreptitiously, including
 23 geolocation data, usernames and communications derived from other SDK applications installed

25 ⁴ See Patti Croft & Catherine McNally, *What Is a Web Beacon and Why Should You Care? All*
 26 *About Cookies* (Sept. 26, 2023), <https://allaboutcookies.org/what-is-a-web-beacon>.

27 ⁵ See Anokhy Desai, *The Half-Baked Future of Cookies and Other Tracking Technologies*, IAPP
 28 (July 2023), <https://iapp.org/resources/article/future-of-cookies-tracking-technologies/>.

29 ⁶ *What Is an SDK? Software Development Kits Explained*, Okta, Inc. (June 30, 2022),
 30 <https://www.okta.com/identify-101/what-is-an-sdk>.

1 on a user's device, and a user's activities within an application after installation.

2 38. All of the information and data captured and collected by third-party trackers,
 3 regardless of the tool used, is capable of being sold and used for marketing and advertising
 4 purposes.

5 **B. Internet Protocol Addresses (“IP Addresses”)**

6 39. One important piece of identifying information collected by third-party trackers is
 7 a website user's IP address. An IP address is a unique identifier for a device. It is written as four
 8 sets of numbers separated by periods – e.g., 123.145.167.189. The first two sets of numbers reflect
 9 what network the device is on. The second two sets of numbers identify the specific device. The
 10 IP address enables a device to communicate with another device, such as a computer's web
 11 browser communicating with a website's server.

12 40. Similar to a telephone number for a person, an IP address is a unique numerical
 13 code associated with a specific internet-connected device on a computer network. The IP
 14 addresses identify all of the devices accessing a given network at any given time.

15 41. Importantly from a privacy perspective, an IP address contains geographical
 16 location information from which the state, city, and zip code of a specific device can be
 17 determined. Given the information that it can and does reveal, an IP address is considered
 18 personally identifiable information and is subject to HIPAA protection.⁷

19 42. Knowing a website user's IP address, and therefore the user's geographic location,
 20 provides “a level of specificity previously unfound in marketing.”⁸ An IP address allows
 21 advertisers to target customers by countries, cities, neighborhoods, and postal codes.⁹ Even more
 22 specifically, it allows advertisers to target specific households, businesses, and even individuals

23
 24
 25
 26 ⁷ See 45 C.F.R. § 164.514(b)(2)(i)(O).

27 ⁸ *IP Targeting: Understanding This Essential Marketing Tool*, AccuData,
 28 <https://www.accudata.com/blog/ip-targeting/> (last visited June 17, 2024).

29 ⁹ *Location-based Targeting That Puts You in Control*, Choozle,
 30 <https://choozle.com/geotargeting-strategies/> (last visited June 17, 2024).

1 with ads that are relevant to their interests.¹⁰

2 43. Indeed, IP targeting is one of the most successful marketing techniques that
3 companies can employ to spread the word about a product or service because companies can use
4 an IP address to identify individuals personally.¹¹ By targeting specific households or businesses,
5 a company can avoid wasting money on ads that are unlikely to be seen by their target audience
6 and can reach their target audience with greater precision.¹² Additionally, by analyzing data on
7 which households or businesses are responding to their ads, IP address targeting can help
8 businesses improve their overall marketing strategies and refine their marketing efforts.¹³

9 44. As alleged below, Defendant installed and continues to install third-party tracker
10 cookies on USA Today website users' browsers. Those trackers have collected and continue to
11 collect browser and device/operating system data as well as identifying and addressing information
12 about Plaintiffs and Class members, including their IP addresses, all without a court order and
13 without those individuals' consent.

14 **C. Defendant's Use of Third-Party Trackers on the USA Today Website**

15 45. Defendant has embedded and implemented several third-party trackers on the USA
16 Today website, including but not limited to (i) Taboola Tracker, (ii) Amobee Tracker, and (iii)
17 Adnx Tracker (the "trackers"). By installing these trackers and their corresponding tracking
18 cookies, Defendant can sell advertising space on the USA Today website. That enables Defendant
19 to monetize its website further and to maximize its revenue by collecting and disclosing/selling
20 user information.

21
22
23
24 ¹⁰ Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov.
25 29, 2023), <https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bfh/>

26 ¹¹ Trey Titone, *The future of IP address as an advertising identifier*, Ad Tech Explained (May 16,
27 2022), <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>

28 ¹² Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov.
29 29, 2023), <https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bfh/>

¹³ *Id.*

1 46. Taboola Tracker is developed by software company Taboola Inc., which uses data
2 analytics to correlate digital content with user preferences across its network of publisher websites.
3 As a content recommendation platform, the Taboola Tracker is designed to collect user data to
4 optimize content suggestions, enhancing both user experience and content monetization for
5 publishers.

6 47. When a website user first accesses and enters the USA Today website, the user's
7 browser sends an HTTP request¹⁴ to Defendant's website server. Defendant's website server sends
8 an HTTP response with directions to load the webpage content and to install the Taboola Tracker
9 on the user's browser. The Taboola Tracker stores a website cookie in the user's browser cache
10 and uses that third-party tracker cookie to collect and share that user's browser and
11 device/operating system data, IP address, and other identifying information with Taboola every
12 time the user interacts with the USA Today website. *See* Figure 1, identifying Taboola,
13 www.usatoday.com, and the user's IP address (45.132.xxx.xxx).

Figure 1:

23 48. This entire process takes place behind the scenes in less than a second. Thus, the
24 Taboola Tracker cookie appears and is implemented the instant the user enters the USA Today
25 website, and it is installed without any further action, clicks, or consent required of the user.

¹⁴ HTTP stands for "HyperText Transfer Protocol." It is the computer communication protocol used for most communication on the world wide web.

1 49. Further, each time a user revisits the USA Today website, the Taboola Tracker
 2 identifies that user and sends the stored website cookie, including the user's browser and
 3 device/operating system data, IP address, and other identifying information, back to Taboola.
 4 ***Even if a user clears the cookies from the user's browser, it makes no difference:*** the next time
 5 that user visits the USA Today website, the Taboola Tracker re-installs the tracker cookie, resets
 6 the tracking process, and resumes transmission of the user's browser and device/operating system
 7 data, IP address, and other identifying information to Taboola on future visits.

8 50. Taboola collects IP addresses to allow it to ascertain a user's location and to target
 9 that user with advertisements tailored to that specific location. According to its website, Taboola
 10 uses its "unique data about people's interests and information consumption to recommend the right
 11 content to the right person at the right time."¹⁵ Taboola assists advertisers with targeting their
 12 campaigns by location, time, browser type, connection type, audience segments, and more.¹⁶

13 51. In addition to the Taboola Tracker, Defendant also embeds the Amobee Tracker on
 14 its USA Today website. Like the Taboola Tracker, the Amobee Tracker is installed the moment a
 15 user accesses the USA Today website, all without any notice to or request for permission from the
 16 user.

17 52. Amobee is a digital marketing technology company that delivers a broad spectrum
 18 of advertising solutions aimed at helping brands, agencies and publishers navigate the digital
 19 landscape. With an ad-serving platform that integrates across various channels such as digital,
 20 social, mobile and video, Amobee delivers targeted advertising content to users based on their
 21 browsing habits and other collected data, *including their IP addresses*. Amobee utilizes HTTP
 22 requests and responses, along with cookies and IP addresses, to track and deliver personalized ads
 23 to users on host sites like USA Today.

24 53. Specifically, when a user visits the USA Today website, an HTTP request is sent
 25
 26

27 ¹⁵ *How Taboola Works*, Taboola Help Center, <https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works> (last visited June 17, 2024).

28 ¹⁶ *Id.*

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

to Amobee's servers. The HTTP request includes the user's IP address and allows Amobee to identify the user's geographic location. Amobee's servers then leverage the information contained within the user's HTTP request to respond with targeted ads tailored to the user.

54. Amobee installs third-party tracker cookies on the user's browser during this process. Those cookies, which also store information regarding the user's browsing behavior, browser and device/operating data, and other identifying information, enable Amobee to recognize the user on subsequent visits to USA Today or to other websites within Amobee's advertising network. They thereby leverage the user's personal data and browsing preferences. *See Figure 2*, identifying Amobee, www.usatoday.com, and the user's IP address (45.132.xxx.xxx).¹⁷

Figure 2:

55. Even if the Amobee Tracker cookies are cleared from the user's browser, the Amobee Tracker is re-installed automatically and instantly on subsequent visits to USA Today. The tracking cycle restarts, ensuring that Amobee consistently receives the user's browser and

¹⁷ The host name “presentation-pdx1.turn.com” signifies the presence of the Amobee tracker. Amobee is the name of the advertising platform, but its tracking cookies use the “turn.com” domain. See <https://www.netify.ai/resources/domains/turn.com>.

1 device/operating system data, IP address, and browsing preferences with every website interaction.
2 This mechanism facilitates a cycle of ad targeting and tracking and increases the relevancy and
3 effectiveness of ads presented by Amobee to users across the web.

4 56. The third tracker embedded in Defendant’s USA Today website is developed by
5 software company Xandr, which Microsoft acquired in 2021. Xandr operates as an advanced
6 advertising company that claims to provide a comprehensive platform for buying and selling
7 consumer-centric digital advertising. The platform, which includes programmatic advertising,
8 data analytics, and cross-screen media solutions, aims to improve the efficiency and effectiveness
9 of advertising across various channels by leveraging data and technology.

10 57. Like other third-party trackers, Xandr allows companies like Defendant to sell
11 advertising space on their websites by using the Adnx Tracker to receive, store and analyze
12 information collected from website visitors. The Adnx Tracker is installed and stored on the user's
13 browser the instant the user enters the USA Today website. The third-party tracker cookie then
14 sends the user's IP address to Xandr each and every time the user interacts with the USA Today
15 website. See Figure 3, identifying Xandr, www.usatoday.com, and the user's IP address
16 (45.132.xxx.xxx).

Figure 3:

28 58. Each of the three trackers embedded on Defendant's USA Today website (1)

1 installs a third-party tracker cookie on users' browsers and (2) captures, collects, and shares with
2 undisclosed third parties USA Today website users' personally identifying and addressing
3 information, including the users' IP addresses, all without users' knowledge or consent.

4 59. Notably, upon information and belief, the trackers collect IP addresses that can be
5 used to ascertain a user's exact location, potentially with precise latitude-longitude coordinates
6 and a zip code. That information can be used by Defendant and third parties to analyze the USA
7 Today website data and conduct targeted advertising based on a user's location as discussed above.

8 60. Further, each of the three trackers embedded on Defendant's USA Today website
9 ***re-installs its tracker cookies every time a user visits the website.*** That happens even if the user
10 previously cleared the cookies from his or her web browser cache. As a result, USA Today website
11 users cannot escape the unauthorized sharing of their personally identifying and addressing
12 information with third-parties Taboola, Amobee, and Xandr.

13 **D. Plaintiffs and Class Members Did Not Consent To Defendant's
14 Disclosure of Their Personally Identifying and Addressing Information,
15 and They Have a Reasonable Expectation of Privacy in Their User Data.**

16 61. Defendant does not ask its USA Today website visitors, including Plaintiffs,
17 whether they consent to having their personally identifying and addressing information disclosed
18 to and used by third parties like Taboola, Amobee, and Xandr. When a website user accesses and
19 enters the USA Today website, there is no pop-up window or other notification to inform users
20 that Defendant is using website tracking technology or installing third-party tracker cookies.

21 62. Additionally, the third-party trackers are incorporated seamlessly – ***and, to users,
22 invisibly*** – in the background on the USA Today website. That seamless and invisible
23 incorporation gave and gives Plaintiffs and Class members no way of knowing that Defendant was
24 collecting their personally identifying and addressing information, including their IP addresses,
25 and secretly sharing that information with undisclosed third parties.

26 63. Further, although the USA Today website does have a Privacy Policy containing
27 some disclosures about how information is collected and shared, that policy can be viewed only
28 after scrolling through all of the website content to the very bottom of the webpage. ***Thus,
Defendant's policies and notices would be seen, if at all, only long after the third-party trackers***

1 ***and cookies had been installed on users' web browsers.***

2 64. In addition to its hard-to-see location, the hyperlink to access the Privacy Policy is
 3 written in small, inconspicuous font and is listed among many other links at the bottom of the USA
 4 Today webpage.

5 65. Unlike first-party cookies that may be technologically necessary to enable a
 6 computer user to view a webpage, third-party tracker cookies are not necessary. Moreover, they

7 (a) simultaneously communicate information to an external server as a user
 8 navigates a website;

9 (b) track users across devices, meaning that a user's actions on multiple devices all
 10 will be included in the information stored regarding that user;

11 (c) are not easily disabled by users; and

12 (d) ***create a record of all of the information that users provide to and/or receive***
 13 ***from the website.***

14 66. Because they were unaware of Defendant's use of third-party trackers and tracking
 15 cookies, Plaintiffs and Class members could not and did not consent to the collection, storage, and
 16 use of their personally identifying and addressing information by undisclosed third parties such as
 17 Taboola, Amobee, and Xandr.

18 67. Plaintiffs and Class members had and have a reasonable expectation of privacy in
 19 their interactions with the USA Today website and their user data, especially their personally
 20 identifying and addressing information. This is even truer of Plaintiffs' and Class members' IP
 21 addresses, which contain geolocation data that can be used to identify, track, and target individuals
 22 in a very specific way.

23 68. Privacy studies, such as those conducted by the *Pew Research Center*, show that
 24 most Americans are concerned about how data is collected about them.¹⁸ Those privacy polls also

25
 26
 27 ¹⁸ Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of*
 28 *Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019),
<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>

1 reflect that Americans consider one of the most important privacy rights to be the need for a
 2 customer or other individual's affirmative consent before a company collects and shares data
 3 regarding that customer or other individual.

4 69. Indeed, according to *Consumer Reports*, more than 90% of Americans believe that
 5 more should be done to ensure that companies protect consumers' privacy. Further, nearly two
 6 thirds of Americans – 64% – believe that companies should be prohibited from sharing data with
 7 third parties, while 63% of Americans want a federal law requiring companies to obtain a
 8 consumer's permission before sharing the consumer's information. To that end, 60% of
 9 Americans believe that companies should be required to be more transparent about their privacy
 10 policies so that consumers can make more informed choices.¹⁹

11 70. Users act in a manner that is consistent with those preferences. During a rollout of
 12 new iPhone operating software, for example, ***94% of U.S. users who were asked for clear,
 13 affirmative consent before allowing companies to track them chose not to share their data.***²⁰

14 71. Defendant's unauthorized (1) installation of third-party tracker cookies on
 15 Plaintiffs' and Class members' web browsers and (2) collection and disclosure to undisclosed third
 16 parties of Plaintiffs' and Class members' personally identifying and addressing information, all
 17 without consent or adequate notification, are invasions of Plaintiffs' and Class members' privacy.

18 72. Plaintiffs and Class members have suffered injuries and damages in the form of (i)
 19 invasion of privacy; (ii) statutory damages; (iii) the continued and ongoing risk to their personally
 20 identifying information that, once out, cannot be restored to its previous level of privacy; and (iv)
 21 the continued and ongoing risk of harassment, spam, and targeted advertisements enabled by the
 22 USA Today website.

23
 24
 25 19 Benjamin Moskowitz et al., *Privacy Front & Center: Meeting the Commercial Opportunity to*
 26 *Support Consumer Rights*, Consumer Reports in collaboration with Omidyar Network (Fall 2020),
https://thedigitalstandard.org/downloads/CR_PrivacyFrontAndCenter_102020_vf.pdf

27 20 See <https://www.wired.co.uk/article/apple-ios14-facebook> ("According to **Flurry Analytics**,
 28 85 per cent of worldwide users clicked 'ask app not to track' when prompted, with the
 proportion rising to 94 per cent in the US.").

CLASS ACTION ALLEGATIONS

73. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and a class (the “USA Today Website Class” or “the Class”) defined as follows:

5 All California residents who, while located within California at any time during the
6 applicable limitations period preceding the original filing of the Complaint in this
7 matter and through and including the date of resolution, accessed and viewed the
8 USA Today website and had their IP addresses and/or browser and device/operating
9 system data collected by and disclosed to the third-party trackers embedded in the
10 USA Today website.

9 74. Excluded from the USA Today Website Class are website users who (i) registered
10 for the USA Today smartphone application and/or (ii) subscribed to receive the USA Today
11 eNewspaper. Employees of Defendant and employees of Defendant’s parents, subsidiaries, and
12 corporate affiliates also are excluded from the Class. Plaintiffs reserve the right to amend or
13 modify the class definition and/or to add sub-classes or limitations to particular issues, where
14 appropriate, based upon subsequently discovered information.

15 75. This action properly may be maintained as a class action under Rule 23 of the
16 Federal Rules of Civil Procedure because (1) there is a well-defined community of interest in the
17 litigation, (2) common questions of law and fact predominate over individual issues, and (3) the
18 proposed Class is ascertainable.

Numerosity

20 76. The USA Today Website Class that Plaintiffs seek to represent contains numerous
21 members and is clearly ascertainable including, without limitation, by using Defendant’s records
22 and/or third-party trackers’ records to determine the size of the Class and to determine the identities
23 of individual Class members.

24 77. Based on information and belief, the USA Today Website Class consists of at least
25 75 individuals. The Class is so numerous that joinder of all members is impracticable.

Typicality

27 78. Plaintiffs’ claims are typical of the claims of all the other members of the USA
28 Today Website Class, as Plaintiffs now suffer and have suffered from the same violations of the

1 law as other putative Class members. Plaintiffs' claims and the Class members' claims are based
2 on the same legal theories and arise from the same unlawful conduct, resulting in the same injury
3 to Plaintiffs and all of the other Class members.

4 **Adequacy**

5 79. Plaintiffs will fairly and adequately represent and protect the interests of the other
6 members of the Class. Plaintiffs have retained competent counsel with substantial experience in
7 prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to
8 prosecuting this action vigorously on behalf of the USA Today Website Class members and have
9 the financial resources to do so. Neither Plaintiffs nor their counsel have any interests that are
10 adverse to those of the other USA Today Website Class members.

11 **Commonality and Predominance**

12 80. By its unlawful actions, Defendant has violated Plaintiffs' and the Class members'
13 rights under the CDAFA, CIPA and the California Constitution. The questions raised are,
14 therefore, of common or general interest to the Class members, who have a well-defined
15 community of interest in the questions of law and fact presented in this Complaint.

16 81. This action involves common questions of law and fact that predominate over any
17 questions affecting only individual Class members. Those common questions of law and fact
18 include, without limitation, the following:

- 19 (a) Whether Plaintiffs and Class members had a reasonable expectation of privacy
20 when they accessed and visited the USA Today website;
- 21 (b) Whether Defendant knowingly and without permission accessed Plaintiffs' and
22 Class members' computers;
- 23 (c) Whether Defendant knowingly and without permission altered, damaged, deleted,
24 destroyed, or otherwise used any data from Plaintiffs' and Class members'
25 computers;
- 26 (d) Whether Defendant knowingly and without permission took, copied, or made use
27 of any data from Plaintiffs' and Class members' computers;
- 28 (e) Whether Defendant knowingly and without permission added, altered, damaged,

deleted, or destroyed any data from Plaintiffs' and Class members' computers;

- (f) Whether Plaintiffs and Class members had a reasonable expectation of privacy in their personally identifying and addressing information, including IP addresses, when they accessed and visited the USA Today website;
- (g) Whether each of the third-party trackers embedded in the USA Today website is a “pen register” under California Penal Code § 638.50(b);
- (h) Whether Defendant has or had a policy or practice of collecting and sharing personally identifying and addressing information collected on the USA Today website including, without limitation, IP addresses and/or browser and device/operating system data, with third-party trackers and/or other third parties;
- (i) Whether Defendant has or had a policy or practice of not disclosing to USA Today website users that it would collect and share their personally identifying and addressing information, including IP addresses and/or browser and device/operating system data, with third-party trackers and/or other third parties;
- (j) Whether Defendant has or had a policy or practice of not obtaining USA Today website users’ prior consent to collect and share personally identifying and addressing information, including IP addresses and/or browser and device/operating system data, with third-party trackers and/or other third parties;
- (k) Whether Defendant sought or obtained a court order for its use of the third-party trackers;
- (l) Whether Defendant’s conduct invaded Plaintiffs’ and Class members’ privacy;
- (m) Whether Defendant’s acts and practices violate or violated California’s Computer Data Access and Fraud Act, Cal. Penal Code § 502;
- (n) Whether Defendant’s acts and practices violate or violated the California Invasion of Privacy Act, Cal. Penal Code § 638.51(a);
- (o) Whether Defendant’s acts and practices violate or violated the California Constitution or individual rights arising under the California Constitution; and

(p) Whether Plaintiffs and Class members are entitled to actual, statutory, nominal, and/or other forms of damages, restitution, and other relief.

Superiority

82. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all of the members of the Class is impracticable and because questions of law and fact common to the USA Today Website Class predominate over any questions affecting only individual members of the Class. Even if every individual member of the Class could afford individual litigation, the court system could not. It would be unduly burdensome to the courts if individual litigation of the numerous cases were to be required. Individualized litigation also would present the potential for varying, inconsistent or contradictory judgments and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the conduct of this action as a class action with respect to some or all of the issues will present fewer management difficulties, conserve the resources of the court system and the parties, and protect the rights of each member of the USA Today Website Class. Further, it will prevent the very real harm that would be suffered by numerous members of the putative Class who simply will be unable to enforce individual claims of this size on their own, and by Defendant's competitors, who will be placed at a competitive disadvantage as their punishment for obeying the law. Plaintiffs anticipate no difficulty in the management of this case as a class action.

83. The prosecution of separate actions by individual members of the USA Today Website Class would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other members of the Class who are not parties to those adjudications or that would substantially impair or impede the ability of those non-party members of the Class to protect their interests.

84. The prosecution of individual actions by members of the USA Today Website Class also would run the risk of establishing inconsistent standards of conduct for Defendant.

FIRST CAUSE OF ACTION
Violation of the California Computer Data Access and Fraud Act
(California Penal Code § 502)

85. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and further allege as follows.

86. The California Legislature enacted the CDAFA with the intent to “expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.” Cal. Penal Code § 502(a).

87. The Legislature further declared that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

88. For purposes of the statute, a number of definitions were provided. The term "access" means to "gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1).

89. The term "computer program or software" is defined as "a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions." Cal. Penal Code § 502(b)(3).

90. The term "computer system" refers to "a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

91. Plaintiffs' and Class members' web browsers used to access the USA Today website are "computer software" and the computers on which Plaintiffs and Class members used

1 their web browsers constitute computers or “computer systems” within the scope of the CDAFA.

2 92. The statute also defines the term “data” to mean a “representation of information, 3 knowledge, facts, concepts, computer software, or computer programs or instructions.” The statute 4 further provides that data may be in “any form, in storage media, or as stored in the memory of the 5 computer or in transit or presented on a display device.” Cal. Penal Code § 502(b)(8).

6 93. As discussed above, a website cookie, including a third-party tracker cookie, and 7 an IP address both are “data” within the meaning of the statute.

8 94. Under California Penal Code § 502(c)(1), it is unlawful knowingly to access and 9 without permission alter, damage, delete, destroy, or otherwise use any data, computer, computer 10 system, or computer network in order to...wrongfully control or obtain money, property or data. 11 Cal. Penal Code § 502(c)(1).

12 95. The statute also makes it unlawful to access knowingly and without permission 13 take, copy, or make use of any data from a computer, computer system, or computer network. Cal. 14 Penal Code § 502(c)(2).

15 96. The CDAFA further prohibits any person from knowingly accessing and without 16 permission adding, altering, damaging, or destroying any data, computer software, or computer 17 programs which reside or exist internal or external to a computer, computer system, or computer 18 network. Cal. Penal Code § 502(c)(4).

19 97. Under subsections (6) and (7) of Penal Code § 502(c), a person also may not 20 knowingly and without permission (i) provide or assist in providing a means of accessing or (ii) 21 access or cause to be accessed any computer, computer system, or computer network. Cal. Penal 22 Code §§ 502(c)(6) and (7).

23 98. Based on Defendant’s unauthorized installation and storage of third-party tracker 24 cookies on Plaintiffs’ and Class members’ web browsers, as alleged above, Defendant knowingly 25 accessed and without permission altered and used Plaintiffs’ and Class members’ data and 26 computer systems in violation of Penal Code § 502(c)(1).

27 99. Similarly, the installation of those third-party tracker cookies violates subsection 28 (c)(4) because Defendant added and altered data and computer software on Plaintiffs’ and Class

1 members' computers or computer systems. Cal. Penal Code § 502(c)(4).

2 100. By installing third-party tracker cookies, Defendant also knowingly and without
3 permission provided those trackers a means of accessing and/or caused to be accessed Plaintiffs'
4 and Class members' computers, computer systems, and/or computer networks in violation of Penal
5 Code §§ 502(c)(6) and (7).

6 101. Further, Defendant's unauthorized collection and disclosure to undisclosed third
7 parties of Plaintiffs' and Class members' personally identifying and addressing information violate
8 Penal Code § 502(c)(2) because Defendant took and made use of data, including IP addresses,
9 from Plaintiffs' and Class members' computers, computer systems, or computer networks.

10 102. Plaintiffs and Class members are residents of California who used their computers,
11 computer systems, and/or computer networks in California. Defendant accessed or caused to be
12 accessed Plaintiffs' and Class members' data and other personally identifying information from
13 within California.

14 103. Defendant was unjustly enriched by accessing, acquiring, taking, and using
15 Plaintiffs' and Class members' data and computer systems without their permission or consent,
16 and using all of that identifying information to maximize revenue from selling advertising space
17 on the USA Today website and for Defendant's own financial benefit. Defendant has been unjustly
18 enriched in an amount to be determined at trial.

19 104. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiffs
20 and Class members have suffered damages. Under Penal Code § 502(e)(1), Plaintiffs and Class
21 members are entitled to compensatory damages, injunctive relief, and other equitable relief in an
22 amount to be determined at trial.

23 105. Plaintiffs and Class members also are entitled to an award of reasonable attorneys'
24 fees and costs under Penal Code § 502(e)(2).

25 **SECOND CAUSE OF ACTION**
26 **Unlawful Use of a Pen Register or Trap and Trace Device**
27 **(California Penal Code § 638.51)**

28 106. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and
further allege as follows.

1 107. The California Legislature enacted the California Invasion of Privacy Act, Cal.
 2 Penal Code §§ 630, *et seq.* (“CIPA”), to address “advances in science and technology [that] have
 3 led to the development of new devices and techniques for the purpose of eavesdropping upon
 4 private communications” and declared “that the invasion of privacy resulting from the continual
 5 and increasing use of such devices and techniques has created a serious threat to the free exercise
 6 of personal liberties and cannot be tolerated in a free and civilized society.” *Id.* § 630. CIPA is
 7 intended “to protect the right of privacy of the people of this state.” *Id.*

8 108. Although CIPA was enacted before the dawn of the Internet, the California
 9 Supreme Court “regularly reads statutes to apply to new technologies where such a reading would
 10 not conflict with the statutory scheme.” *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal.
 11 Sept. 26, 2013); *see also Greenley*, 2023 WL 4833466, at *15 (**referencing CIPA’s “expansive
 12 language” when finding that software was a “pen register”**); *Javier v. Assurance IQ, LLC*, 2022
 13 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, [CIPA]
 14 Section 631(a) applies to Internet communications.”). This is consistent with the observation in
 15 *Matera v. Google Inc.* that, “when faced with two possible interpretations of CIPA, the California
 16 Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest
 17 privacy protection.” *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

18 109. Particularly pertinent here, California Penal Code § 638.51(a) makes it unlawful
 19 for a person to “install or use a pen register or a trap and trace device without first obtaining a court
 20 order.”

21 110. A “pen register” is “a device or process that records or decodes dialing, routing,
 22 addressing, or signaling information transmitted by an instrument or facility from which a wire or
 23 electronic communication is transmitted, but not the contents of a communication.” Cal. Penal
 24 Code § 638.50(b).

25 111. A “trap and trace device” is a “a device or process that captures the incoming
 26 electronic or other impulses that identify the originating number or other dialing, routing,
 27 addressing, or signaling information reasonably likely to identify the source of a wire or electronic
 28 communication, but not the contents of a communication.” Cal. Penal Code § 638.50(c).

1 112. In essence, a “pen register” is a “device or process” that records *outgoing*
 2 information, while a “trap and trace device” is a “device or process” that records *incoming*
 3 information. For example, if a user sends an email, a “pen register” might record the email address
 4 from which the email was sent, the email address to which the email was sent, and the subject line
 5 – because this is the user’s *outgoing* information. On the other hand, if that same user receives an
 6 email, a “trap and trace device” might record the email address from which that email was sent,
 7 the email address to which it was sent, and the subject line – because this is *incoming* information
 8 that is being sent to that same user.

9 113. The three trackers embedded in the USA Today website – Taboola, Amobee, and
 10 Adnx – are “pen registers” because each of them is a device or process that captures and records
 11 outgoing addressing or signaling information from the electronic communications transmitted by
 12 Plaintiffs’ and Class members’ computers, computer systems, and computer networks as they are
 13 accessing and visiting the USA Today website.

14 114. At all relevant times, Defendant installed and is installing each of the three pen
 15 register trackers on Plaintiffs’ and Class members’ web browsers in California and used the
 16 trackers to collect Plaintiffs’ and Class members’ outgoing IP addresses and/or browser and
 17 device/operating system data. IP addresses constitute addressing information and do not
 18 necessarily reveal any more about the underlying contents of the communication. *In re Zynga*
 19 *Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014).

20 115. Unaware of Defendant’s installation and use of the third-party trackers as pen
 21 registers, Plaintiffs and Class members could not have provided and did not provide their prior
 22 consent to Defendant’s installation or use of the third-party trackers or pen registers.

23 116. Upon information and belief, Defendant was not authorized by any court order to
 24 use a pen register to track Plaintiffs’ and Class members’ location data and other identifying or
 25 addressing information.

26 117. Defendant’s conduct as described above violated California Penal Code § 638.51.
 27 As a result, Defendant is liable for the relief sought by Plaintiffs and the USA Today Website
 28 Class. Under California Penal Code § 637.2, Plaintiffs and Class Members are entitled to and seek

1 statutory damages of \$5,000 for each of Defendant's numerous CIPA violations.

2 **THIRD CAUSE OF ACTION**

3 **Invasion of Privacy**
(Violation of Art. 1, § 1, California Constitution)

4 118. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and
5 further allege as follows.

6 119. "Privacy" is listed in Article I, Section 1, of the California Constitution as a
7 fundamental right of all Californians. That section of the Constitution provides as follows: "All
8 people are by nature free and independent and have inalienable rights. Among these are enjoying
9 and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and
10 obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

11 120. The right to privacy in California's Constitution creates a right of action against
12 private entities such as Defendant. To state a claim for invasion of privacy under the California
13 Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable
14 expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential
15 impact as to constitute an egregious breach of social norms.

16 121. Plaintiffs and Class members have a legally protected privacy interest in their
17 personally identifying information and addressing information that are captured, without notice or
18 consent, when they access and view the USA Today website. These privacy interests are
19 recognized by the California Constitution, CDAFA, CIPA, HIPAA, and numerous other statutes.

20 122. Plaintiffs and Class members had a reasonable expectation of privacy under the
21 circumstances, as they could not reasonably have expected that Defendant would violate state and
22 federal privacy laws. Plaintiffs and Class members were not aware of and could not reasonably
23 have expected that Defendant would use website tracking technology and install third-party tracker
24 cookies without notice and/or without obtaining consent. Those unauthorized trackers collected
25 and transmitted to undisclosed third parties Plaintiffs' and Class members' personally identifying
26 and addressing information, including their IP addresses, which contain geolocation data.

27 123. Defendant's unauthorized (1) installation of third-party tracker cookies and (2)
28 collection and disclosure to undisclosed third parties of Plaintiffs' and Class members' personally

1 identifying and addressing information, all without consent or adequate notification to Plaintiffs
2 and Class members, are invasions of Plaintiffs' and Class members' privacy.

3 124. Defendant's conduct constituted a serious invasion of privacy that would be highly
4 offensive to a reasonable person in that (i) the information disclosed by Defendant and shared with
5 third-party trackers was personally identifying information protected by the California
6 Constitution and numerous California and federal statutes; (ii) Defendant did not have
7 authorization or consent to disclose that personally identifying and addressing information,
8 including IP addresses, to any third-party tracker embedded in the USA Today website, and the
9 trackers did not have authorization to collect and use that geolocation information; and (iii) the
10 invasion deprived Plaintiffs and Class members of the ability to control the dissemination and
11 circulation of that information, an ability that is a fundamental privacy right. Defendant's conduct
12 constitutes a severe and egregious breach of social norms.

13 125. As a direct and proximate result of Defendant's actions, Plaintiffs and Class
14 members have had their privacy invaded and have sustained injury, including injury to their peace
15 of mind.

16 126. Plaintiffs and USA Today Website Class members seek appropriate relief for that
17 injury, including but not limited to restitution, disgorgement of profits earned by Defendant
18 because of, by way of or in connection with the intrusions upon Plaintiffs' and Class members'
19 privacy, nominal damages, and all other equitable relief that will compensate Plaintiffs and Class
20 members properly for the harm to their privacy interests.

21 127. Plaintiffs also seek such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

23 **WHEREFORE**, Plaintiffs, on behalf of themselves and the members of the Class, pray
24 for the following relief:

25 a. An order certifying the USA Today Website Class, appointing Plaintiffs Ryan Wu
26 and Saber Khamooshi as representatives of the USA Today Website Class, and
27 appointing counsel for Plaintiffs as counsel for the USA Today Website Class;

- b. An order declaring that Defendant's actions, as described above, violate California Penal Code § 502;
- c. An order declaring that Defendant's actions, as described above, violate California Penal Code § 638.51;
- d. An order declaring that Defendant's actions, as described above, violate Art. 1, § 1 of the California Constitution;
- e. A judgment for and award of compensatory damages or other equitable relief under California Penal Code § 502(e)(1) to Plaintiffs and each of the members of the USA Today Website Class;
- f. A judgment for and award of statutory damages of \$5,000 per violation of CIPA under California Penal Code § 637.2 to Plaintiffs and each of the members of the USA Today Website Class;
- g. A judgment for and award of restitution, disgorgement of profits, and nominal damages to which Plaintiffs and each of the members of the USA Today Website Class are entitled by law;
- h. Payment of costs of the suit;
- i. Payment of attorneys' fees under California Code of Civil Procedure § 1021.5 and Penal Code § 502(e)(2);
- j. An award of pre- and post-judgment interest to the extent allowed by law; and
- k. Such other and further relief as the Court may deem proper.

Respectfully submitted,

Dated: October 8, 2024

KELLER GROVER LLP

By: 
ERIC A. GROVER
Attorneys for Plaintiffs

1 **JURY DEMAND**

2 Plaintiffs request a trial by jury of all claims that can be so tried.

3

4

5 Respectfully submitted,

6

Dated: October 8, 2024

KELLER GROVER LLP

7

8 By: 

9
10 ERIC A. GROVER
11 *Attorneys for Plaintiffs*

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28